

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-306026

(43)Date of publication of application : 02.11.2000

(51)Int.Cl.

G06F 19/00

G06F 12/00

G06F 13/00

G06F 17/30

(21)Application number : 11-114894

(71)Applicant : HITACHI LTD

(22)Date of filing : 22.04.1999

(72)Inventor : HASHIMOTO HIROBUMI

MURATA TOMOHIRO

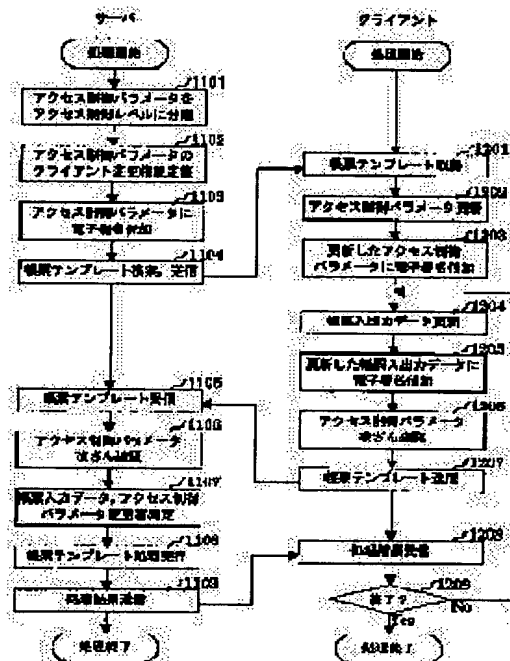
YOKOMURA KATSUYA

(54) ELECTRONIC DOCUMENT PROCESSING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent illegal transactions of a user in an electronic commercial transaction with an electronic document.

SOLUTION: Concerning an electronic document template, in a server, an access control parameter for controlling the read and update of input items on the document and records in a job database is separated to a server definition parameter and a user definition parameter (1101). The hash values of the respective parameters are found, enciphered signatures are added (1103), and the template is transmitted corresponding to the request of a client. When the parameter is updated (1202) at the client side, processing similar to 1103 is performed (1203), data are inputted (1204), processing similar to 1103 is performed to the data (1205), the hash value of the parameter is found, falsification of the parameter is confirmed on the basis of the result compounding this hash value and the signature (1206), and the template is transmitted to the server (1207). In the server, the falsification is confirmed similarly to the server, processing is performed to the template and the result is returned to the client.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-306026

(P2000-306026A)

(43) 公開日 平成12年11月2日 (2000. 11. 2)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 19/00		G 0 6 F 15/22	N 5 B 0 7 5
12/00	5 3 7	12/00	5 3 7 A 5 B 0 8 2
	5 4 6		5 3 7 H 5 B 0 8 9
	3 5 1		5 4 6 T
13/00		13/00	3 5 1 Z

審査請求 未請求 請求項の数 5 O L (全 13 頁) 最終頁に続く

(21) 出願番号 特願平11-114894

(22) 出願日 平成11年4月22日 (1999. 4. 22)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 橋本 博文

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 村田 智洋

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100099298

弁理士 伊藤 修 (外1名)

最終頁に続く

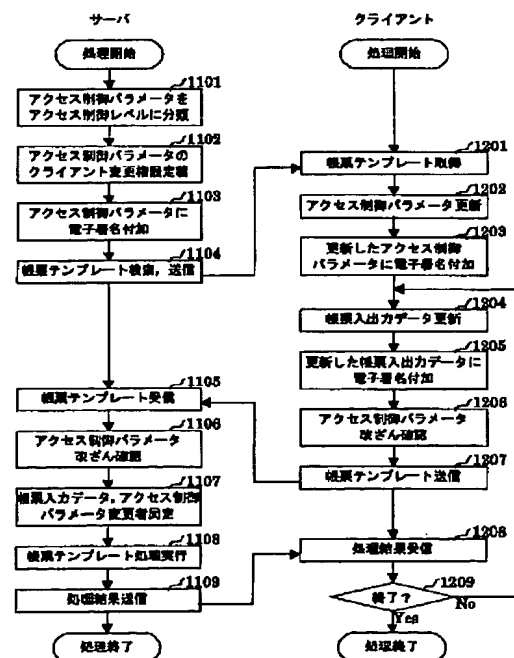
(54) 【発明の名称】 電子帳票処理方法

(57) 【要約】

【課題】 電子帳票による電子商取引で、ユーザの不正な取り引きを防止する。

【解決手段】 サーバにおいて電子帳票テンプレートに対し、帳票の入力項目と業務データベースのレコードの読み出しと更新を制御するアクセス制御パラメータをサーバ定義パラメータと、ユーザ定義パラメータに分け(1101)、各パラメータのハッシュ値を求め暗号化した署名を付加し(1103)、クライアントの要求に応じてテンプレートを送信し(1104 1201)、クライアントではパラメータが更新されたら(1202)、1103と同様の処理をし(1203)、データを入力し(1204)、データに対し1103と同様の処理をし(1205)、パラメータのハッシュ値を求め、これと前記署名を複合化したものに基づきパラメータの改ざんを確認し(1206)、テンプレートをサーバに送信し(1207)、サーバでは1206と同様に改ざんを確認し、テンプレートに対する処理をし、結果をクライアントに返す。

【図1】



【特許請求の範囲】

【請求項 1】 サーバとクライアントを有する電子帳票処理システムにおいて、電子帳票における入出力項目と、当該入出力項目に表示または入力されるデータを格納する業務データベースのレコードとの対応づけを記憶した電子帳票テンプレートにしたがい、電子帳票の入出力項目に表示または入力されるデータに関連して当該電子帳票の入出力項目に対応する業務データベースのレコードの読出しまたは更新を行う電子帳票処理方法であって、

当該電子帳票への入出力項目に対応する業務データベースのデータレコードの読出しと更新を制御するパラメータ情報（アクセス制御パラメータ情報）を前記電子帳票テンプレートに記憶し、

当該アクセス制御パラメータ情報に対する参照、更新の権限を、セキュリティポリシーに従い1つ以上の管理レベル（アクセス制御レベル）に設定し、

当該アクセス制御レベルを示す識別コードをタグコード（セキュリティタグコード）として当該アクセス制御パラメータに付加し、

特定の該セキュリティタグコードが付加されたアクセス制御パラメータ値またはパラメータ値の集合に対して一方向ハッシュ関数を用いたハッシュ値を生成することを特徴とする電子帳票処理方法。

【請求項 2】 請求項 1 記載の電子帳票処理方法において、

サーバは、前記生成したハッシュ値を記憶した後、当該電子帳票テンプレートをクライアントの要求に応じてクライアントに送付し、

クライアントは、送付された電子帳票テンプレートを基に電子帳票テンプレートの入出力項目に対するデータの入力要求またはデータの表示要求（あわせてデータアクセス要求と呼ぶ）を当該電子帳票テンプレートに記録した後、当該電子帳票テンプレートをサーバに送付し、

サーバは、受け取った電子帳票テンプレートに記憶されている特定のセキュリティタグコードが付加されたアクセス制御パラメータ値またはパラメータ値の集合のハッシュ値を生成し、予めサーバで記憶した当該電子帳票テンプレートのハッシュ値と比較し、当該電子帳票テンプレートに記憶された、特定のセキュリティタグコードが付加されたアクセス制御パラメータ値またはパラメータ値の内容が改ざんされていないことを確認した後、当該電子帳票テンプレートに記憶されたアクセス要求に基づき、当該電子帳票への入出力項目に対応する業務データベースのデータレコード読出し、または、更新を行うことを特徴とする電子帳票処理方法。

【請求項 3】 サーバとクライアントを有する電子帳票処理システムにおいて、電子帳票における入出力項目と、当該入出力項目に表示または入力されるデータを格納する業務データベースのレコードとの対応づけを記憶

した電子帳票テンプレートにしたがい、電子帳票の入出力項目に表示または入力されるデータに関連して当該電子帳票の入出力項目に対応する業務データベースのレコードの読出しまたは更新を行う電子帳票処理方法であって、

当該電子帳票への入出力項目に対応する業務データベースのデータレコードの読出しと更新を制御するパラメータ情報（アクセス制御パラメータ情報）を前記電子帳票テンプレートに記憶し、

10 当該アクセス制御パラメータ情報に対する参照、更新の権限を、セキュリティポリシーに従い1つ以上の管理レベル（アクセス制御レベル）に設定し、

当該アクセス制御レベルを示す識別コードをタグコード（セキュリティタグコード）として当該アクセス制御パラメータに付加し、

クライアントの特定のユーザに対して特定のセキュリティタグコードが付加されたアクセス制御パラメータ値またはパラメータ値に対する変更権限を付与し、

20 サーバは、該変更権限を付与されたユーザの ID と該ユーザが提供する公開暗号鍵を記憶した後、電子帳票テンプレートをクライアント側の要求に応じてクライアントに送付し、

クライアント側は、当該電子帳票テンプレートのセキュリティタグコードを参照して、特定のセキュリティタグコード付けされたアクセス制御パラメータ値またはパラメータ値の集合に対する更新を行い、更新者が有する秘密鍵を用いて特定のタグ付けされたアクセス制御パラメータ値またはパラメータ値の集合に電子署名を生成し、生成した電子署名を電子帳票テンプレートに付加し、さらに、当該電子帳票テンプレートに関するデータアクセス要求を設定して当該電子帳票テンプレートをサーバに送付し、

30 サーバは、当該電子帳票テンプレートを送付してきたクライアント側ユーザが提供している公開暗号鍵を用いて当該電子帳票テンプレートの電子署名を解読することにより、特定タグ付けされたアクセス制御パラメータ更新に関するクライアント側での更新者をサーバ側で同定し、当該特定セキュリティタグ付けされたアクセス制御パラメータの値については改ざんチェックを省略することを特徴とする電子帳票処理方法。

40 【請求項 4】 サーバとクライアントを有する電子帳票処理システムにおいて、電子帳票における入出力項目と、当該入出力項目に表示または入力されるデータを格納する業務データベースのレコードとの対応づけを記憶した電子帳票テンプレートにしたがい、電子帳票の入出力項目に表示または入力されるデータに関連して当該電子帳票の入出力項目に対応する業務データベースのレコードの読出しまたは更新を行う電子帳票処理方法であって、

50 前記サーバは、前記電子帳票テンプレートに定義されて

いる電子帳票の各入出力項目の集合を識別するためのタグ情報を電子帳票テンプレートに付加し、当該電子帳票への入出力項目に対応する業務データベースのデータレコードの読出しと更新を制御するタグ記述されたアクセス制御パラメータ情報に対する参照、更新権限を、セキュリティポリシーに従い、1つ以上のアクセス制御レベルに分類し、当該アクセス制御レベルを示す属性を、セキュリティタグコードとして前記電子帳票テンプレートに定義し、前記セキュリティタグコードを用いて、特定のタグ付けされた電子帳票入出力データまたはアクセス制御パラメータに対してサーバ側で電子署名を前記電子帳票テンプレートに付加して、特定のタグ付けされた電子帳票入出力データまたはアクセス制御パラメータに対する変更権限をクライアントの特定のユーザに付与した後、該電子帳票テンプレートをクライアント側の要求に応じてクライアントに送付し、クライアント側では、セキュリティタグコードを参照して、特定のタグ付けされたアクセス制御パラメータの更新あるいは電子帳票入出力データの内容の更新を行い、更新者の電子署名を電子帳票テンプレートに付加し、該更新者の電子署名と、サーバ側で行った電子帳票テンプレートの特定のタグ付けされた電子帳票入出力データまたはアクセス制御パラメータに対する電子署名に基づき、特定のタグ付き電子帳票定義データの内容が改ざんされていないか確認し、電子帳票テンプレートをサーバに送付する前にクライアント側で、更新者の同定を可能にすることを特徴とする電子帳票処理方法。

【請求項5】 請求項1乃至請求項4のいずれかの請求項記載の電子帳票処理方法において、

前記アクセス制御パラメータは、前記クライアント側のユーザが変更することのできないサーバ定義パラメータと、前記サーバから変更権限を付与された前記クライアント側のユーザが自由に変更することのできるユーザ定義パラメータを有することを特徴とする電子帳票処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子帳票処理方法に係わり、ユーザの入力ミスや不正入力のチェックを行えるようにし、また、データの不正な改ざんを防止することを可能にする電子帳票処理方法に関する。

【0002】

【従来の技術】通信ネットワークを介した電子帳票処理方法として、インターネットを利用した電子帳票処理方法が注目されている。これは、クライアント側で入力したデータをサーバ側に送り、サーバはデータベースなどと連携して処理を行い、結果をクライアント側に出力する方法である。サーバとデータベースとの連携には、CGI(Common Gateway Interface)を利用したものが一般的である。CGIとはサーバと外部プログラムとのイ

ンタフェースを定義したものであるが、これを利用したCGIプログラムにより、サーバとデータベースなどの外部システムとの連携が可能になる。

【0003】「イントラネットのためのオブジェクト指向データベース技術」(ソフト・リサーチ・センター社発行、大磯和宏他著)の141ページから184ページによると、具体的な手順は、以下の通りである。

① webブラウザからのWebサーバへCGIプログラム起動要求

② webサーバがCGIプログラムを起動してパラメータを渡す

③ CGIプログラムがデータベースシステムにアクセスする

④ データベースシステムから検索や更新の結果やアクションがCGIプログラムに返される

⑤ CGIプログラムが結果をHTMLにしてWebサーバの標準出力に返す

⑥ WebサーバがCGIプログラムの出力をWebブラウザに転送する

ここで、ユーザの要求からデータやシステムの機密性や保全性を保証するために、CGIプログラムでユーザの不正な要求を排除したり、Webサーバやデータベースシステムのアクセス管理を行うことにより、Webサーバやデータベースシステムに対する不正なアクセスや改ざんを防止している。また、ダウンロードプログラムをサーバからクライアントにインストールすることで、ユーザの不正な要求を、クライアント側で防止する方法もある。

【0004】

【発明が解決しようとする課題】しかしながら、CGIプログラムでは、ユーザの入力はサーバ側で処理されるので、単純な入力ミスや入力漏れなども一度サーバ側に送信して、初めてエラーを検出してもう一度クライアントに送り返して、入力を受け付けるという方法を取るため、通信のオーバーヘッドが多くなる。また、CGIプログラムを起動するフォームはユーザ側で勝手に作成して、送信することも可能なので、ユーザが起こしうる全ての不正アクセスを想定し、CGIプログラム側でフィルタリングを行わなければならない。ダウンロードプログラムをクライアント側にインストールして、ユーザの不正入力をクライアント側で防止する方法に関しても、種類の異なる帳票毎にプログラムを作成して管理するにはコストがかかる。また、この方法でもユーザがプログラムを勝手に作成してデータをサーバへ送信することが可能である。さらに、前記のCGIプログラムを用いる方法でも、ダウンロードプログラムを用いる方法でも、基本的にプログラムベースで管理を行っているので、処理方法に変更を加える場合にその管理コストが大きくなる。

【0005】本発明の目的は、前記従来技術の問題点を

解決し、電子帳票処理のために必要なアプリケーションの数を減少させ、さらに処理手順の変更に対して、柔軟に対処し、またユーザの入力ミスによるサーバとクライアントとの通信のオーバーヘッドを減少させながら、ユーザの不正な取り引きを防止することができる電子帳票処理方法を提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するために、本発明は、サーバとクライアントを有する電子帳票処理システムにおいて、電子帳票における入出力項目と、当該入出力項目に表示または入力されるデータを格納する業務データベースのレコードとの対応づけを記憶した電子帳票テンプレートにしたがい、電子帳票の入出力項目に表示または入力されるデータに関連して当該電子帳票の入出力項目に対応する業務データベースのレコードの読出しまたは更新を行う電子帳票処理方法であり、当該電子帳票への入出力項目に対応する業務データベースのデータレコードの読出しと更新を制御するパラメータ情報（アクセス制御パラメータ情報）を前記電子帳票テンプレートに記憶し、当該アクセス制御パラメータ情報に対する参照、更新の権限を、セキュリティポリシーに従い1つ以上の管理レベル（アクセス制御レベル）に設定し、当該アクセス制御レベルを示す識別コードをタグコード（セキュリティタグコード）として当該アクセス制御パラメータに付加し、特定の該セキュリティタグコードが付加されたアクセス制御パラメータ値またはパラメータ値の集合に対して一方向ハッシュ関数を用いたハッシュ値を生成するようにしている。

【0007】さらに、サーバは、前記生成したハッシュ値を記憶した後、当該電子帳票テンプレートをクライアントの要求に応じてクライアントに送付し、クライアントは、送付された電子帳票テンプレートを基に電子帳票テンプレートの入出力項目に対するデータの入力要求またはデータの表示要求（あわせてデータアクセス要求と呼ぶ）を当該電子帳票テンプレートに記録した後、当該電子帳票テンプレートをサーバに送付し、サーバは、受け取った電子帳票テンプレートに記憶されている特定のセキュリティタグコードが付加されたアクセス制御パラメータ値またはパラメータ値の集合のハッシュ値を生成し、予めサーバで記憶した当該電子帳票テンプレートのハッシュ値と比較し、当該電子帳票テンプレートに記憶された、特定のセキュリティタグコードが付加されたアクセス制御パラメータ値またはパラメータ値の内容が改ざんされていないことを確認した後、当該電子帳票テンプレートに記憶されたアクセス要求に基づき、当該電子帳票への入出力項目に対応する業務データベースのデータレコード読出し、または、更新を行うようにしている。

【0008】また、サーバとクライアントを有する電子帳票処理システムにおいて、電子帳票における入出力項

目と、当該入出力項目に表示または入力されるデータを格納する業務データベースのレコードとの対応づけを記憶した電子帳票テンプレートにしたがい、電子帳票の入出力項目に表示または入力されるデータに関連して当該電子帳票の入出力項目に対応する業務データベースのレコードの読出しまたは更新を行う電子帳票処理方法であり、当該電子帳票への入出力項目に対応する業務データベースのデータレコードの読出しと更新を制御するパラメータ情報（アクセス制御パラメータ情報）を前記電子帳票テンプレートに記憶し、当該アクセス制御パラメータ情報に対する参照、更新の権限を、セキュリティポリシーに従い1つ以上の管理レベル（アクセス制御レベル）に設定し、当該アクセス制御レベルを示す識別コードをタグコード（セキュリティタグコード）として当該アクセス制御パラメータに付加し、クライアントの特定のユーザに対して特定のセキュリティタグコードが付加されたアクセス制御パラメータ値またはパラメータ値に対する変更権限を付与し、サーバは、該変更権限を付与されたユーザのIDと該ユーザが提供する公開暗号鍵を記憶した後、電子帳票テンプレートをクライアント側の要求に応じてクライアントに送付し、クライアント側は、当該電子帳票テンプレートのセキュリティタグコードを参照して、特定のセキュリティタグコード付けされたアクセス制御パラメータ値またはパラメータ値の集合に対する更新を行い、更新者が有する秘密鍵を用いて特定のタグ付けされたアクセス制御パラメータ値またはパラメータ値の集合に電子署名を生成し、生成した電子署名を電子帳票テンプレートに付加し、さらに、当該電子帳票テンプレートに関するデータアクセス要求を設定して当該電子帳票テンプレートをサーバに送付し、サーバは、当該電子帳票テンプレートを送付してきたクライアント側ユーザが提供している公開暗号鍵を用いて当該電子帳票テンプレートの電子署名を解読することにより、特定タグ付けされたアクセス制御パラメータ更新に関するクライアント側での更新者をサーバ側で同定し、当該特定セキュリティタグ付けされたアクセス制御パラメータの値については改ざんチェックを省略するようにしている。

【0009】また、サーバとクライアントを有する電子帳票処理システムにおいて、電子帳票における入出力項目と、当該入出力項目に表示または入力されるデータを格納する業務データベースのレコードとの対応づけを記憶した電子帳票テンプレートにしたがい、電子帳票の入出力項目に表示または入力されるデータに関連して当該電子帳票の入出力項目に対応する業務データベースのレコードの読出しまたは更新を行う電子帳票処理方法であり、前記サーバは、前記電子帳票テンプレートに定義されている電子帳票の各入出力項目の集合を識別するためのタグ情報を電子帳票テンプレートに付加し、当該電子帳票への入出力項目に対応する業務データベースのデータレコードの読出しと更新を制御するタグ記述されたア

アクセス制御パラメータ情報に対する参照、更新権限を、セキュリティポリシーに従い、1つ以上のアクセス制御レベルに分類し、当該アクセス制御レベルを示す属性を、セキュリティタグコードとして前記電子帳票テンプレートに定義し、前記セキュリティタグコードを用いて、特定のタグ付けされた電子帳票入出力データまたはアクセス制御パラメータに対してサーバ側で電子署名を前記電子帳票テンプレートに付加して、特定のタグ付けされた電子帳票入出力データまたはアクセス制御パラメータに対する変更権限をクライアントの特定のユーザに付与した後、該電子帳票テンプレートをクライアント側の要求に応じてクライアントに送付し、クライアント側では、セキュリティタグコードを参照して、特定のタグ付けされたアクセス制御パラメータの更新あるいは電子帳票入出力データの内容の更新を行い、更新者の電子署名を電子帳票テンプレートに付加し、該更新者の電子署名と、サーバ側で行った電子帳票テンプレートの特定のタグ付けされた電子帳票入出力データまたはアクセス制御パラメータに対する電子署名に基づき、特定のタグ付き電子帳票定義データの内容が改ざんされていないか確認し、電子帳票テンプレートをサーバに送付する前にクライアント側で、更新者の同定を可能にするようにしている。

【0010】また、前記アクセス制御パラメータは、前記クライアント側のユーザが変更することのできないサーバ定義パラメータと、前記サーバから変更権限を付与された前記クライアント側のユーザが自由に変更することのできるユーザ定義パラメータを有するようにしている。

【0011】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。図1は、本発明の実施の形態を示す処理フロー図である。図2は、本実施の形態を実現するための装置構成を含む電子帳票処理システムの全体構成図である。図3は、本実施の形態を実現するための、サーバ装置のモジュール構成である。図4は、本実施の形態を実現するための、クライアント装置のモジュールである。

【0012】まず、図2に示す電子帳票処理システムの全体構成図について説明する。

【0013】本実施形態の電子帳票処理システムは、電子帳票処理を管理するサーバ11と電子帳票の入力を行うクライアント12とが、通信ネットワーク13で連結されたシステムである。サーバ11の装置構成は、計算機111に、記憶装置112、業務データベース113、通信ケーブル114を接続したものである。クライアント12の装置構成は、計算機122に、入力装置121、表示装置123、記憶装置124、通信ケーブル125を接続したものである。

【0014】図3は、サーバ11のモジュール構成である。計算機111は、通信機構21、処理機構22、解

析機構23、データベース管理機構24で構成されている。なお、サーバに付随する入力装置、出力装置（表示装置）等の記載は図示省略している。通信機構21は、クライアント12と通信を行うためのものである。解析機構23は、電子帳票の処理手順を記述した帳票テンプレートの解析を行うものである。処理機構22は、解析機構23が解析した帳票テンプレートに対する処理を実行するものである。データベース処理機構24は、処理機構22で処理する帳票テンプレートをもとに、業務データベース113のデータの読み出しと更新を行うものである。記憶装置112は、帳票テンプレートの保存や、帳票処理で用いる暗号／復号ライブラリの保存、アクセス制御パラメータのハッシュ値の保存を行うものである。

【0015】図4は、クライアント12のモジュール構成である。計算機122は、通信機構31、処理機構32、解析機構33で構成されている。通信機構31は、電子帳票処理サーバ11と通信を行うためのものである。解析機構33は、電子帳票の処理手順を記述した帳票テンプレートの解析を行うものである。処理機構32は、解析機構33が解析した帳票テンプレートに対する処理を実行するものである。記憶装置124は、帳票処理で用いる暗号／復号ライブラリの保存や表示機構123に帳票の入力画面を表示するためのGUI（Graphical User Interface）ライブラリの保存を行うものである。

【0016】図5は、帳票テンプレート41の構成図である。まず、図5に示す、帳票テンプレート41の構成図について説明する。帳票テンプレート41は、タグ付き文字データで記述される。1行目<帳票テンプレート>は帳票テンプレートの開始タグで、帳票テンプレート41の情報の開始を示している。最終行である18行目の</帳票テンプレート>は、帳票テンプレートの終了タグであり、帳票テンプレート41の情報の終了を示している。すなわち、帳票テンプレートの開始タグと終了タグで挟まれた、2行目から17行目が帳票テンプレートタグの値であり、帳票テンプレート41の内容である。帳票テンプレート41は、データ領域411、アクセス制御パラメータ412、文書保護情報413で構成される。

【0017】データ領域411は、ユーザの入力内容を帳票の入力項目毎に保存する領域である。図5の例では、2行目のデータ領域開始タグ<データ領域>と6行目のデータ領域終了タグ</データ領域>に挟まれた、3行目から5行目がデータ領域の内容である。データ領域411では、帳票における入力項目毎に対応するタグを割り振り、ユーザの入力したデータに対応するタグの値として保存する。図5では、この帳票の入力項目は、商品名と数量と配送先であり、まだユーザは何も入力していないので、どのタグも値がないが、例えばユーザが

商品名をディスプレイと入力したら、3行目は<商品名>ディスプレイ</商品名>となる。

【0018】アクセス制御パラメータ412は、サーバ定義パラメータ414、ユーザ定義パラメータ415で構成される。アクセス制御パラメータ412は、データ領域411の入力項目と業務データベース113のデータレコードとの対応づけと、データ領域411の入力項目データと対応する業務データベース113のデータレコードの読み出し及び更新とを制御するパラメータ情報（アクセス制御情報）を記述するものである。サーバ定義パラメータ414は、アクセス制御パラメータ412で定義されるアクセス制御パラメータの内、電子帳票処理サーバ11で定義され、電子帳票処理クライアント12のユーザは変更できないアクセス制御パラメータを定義するものである。ユーザ定義パラメータ415は、アクセス制御パラメータ412で定義されるアクセス制御パラメータの内、サーバから変更権限を与えられた電子帳票処理クライアント12のユーザが自由に変更できる、アクセス制御パラメータを定義するものである。

【0019】文書保護情報413は、アクセスパラメータ保護情報416、データ保護情報417で構成される。文書保護情報413は、アクセス制御パラメータ412やデータ領域411の不正な改ざんを防止するために、アクセス制御パラメータ412やデータ領域411の定義者または変更者の署名を保存するものである。

【0020】アクセス制御パラメータ保護情報416は、アクセス制御パラメータ412の不正な改ざんを防止するために、アクセス制御パラメータ412の定義者または変更者の署名を保存する。アクセス制御パラメータ保護情報416は、サーバ定義パラメータ保護情報418、ユーザ定義パラメータ保護情報419で構成される。サーバ定義パラメータ保護情報418は、サーバ定義パラメータ414が帳票処理クライアント12のユーザによって改ざんされないように、帳票処理サーバの署名を保存するものである。ユーザ定義パラメータ保護情報419は、ユーザ定義パラメータ415が帳票処理クライアント12のユーザによって変更されたときに、変更を行ったユーザを特定するために変更を行ったユーザの署名を保存するものである。データ保護情報417は、データ領域411が帳票処理クライアント12のユーザによって変更されたときに、同一のユーザが変更を行った入力項目とその内容に対しての当該ユーザの署名を保存するものである。

【0021】図6は、本実施形態により作成された文書テンプレート41のアクセス制御パラメータ412を示す。図7は、本実施形態により作成された文書テンプレート41の文書保護情報413を示す。図8は、本実施形態により作成された、アクセス制御パラメータ412のテーブル構成図である。アクセス制御パラメータ412は、入力項目名511毎に、入力データ型を示すデー

タ型512、入力の際有効なデータの情報が格納されているデータベースを指定する入力DB513、入力の際有効なデータの情報が格納されているデータベースのレコードを指定する入力レコード514、ユーザの入力したデータを格納する業務データベース113のデータベース名を指定する出力DB515、ユーザの入力したデータのデータの情報を格納する業務データベースのレコードを示す出力レコード516で構成される。

【0022】次に、図2、図3、図4及び、図5、図6、図7、図8を引用しながら、図1のフロー図に従って、本実施形態の処理動作を説明する。ステップ1101では、まず、サーバ11の計算機111の処理機構22に新規帳票テンプレート41を作成する。図8で示しているアクセス制御パラメータ412に対する参照、更新権限を、セキュリティポリシーに従って、1つ以上のアクセス制御レベルに分類して、このアクセス制御レベルの内の1つに対応するクライアント12のユーザが変更できない情報をサーバ定義パラメータ414に、また、アクセス制御レベルの内の他の1つに対応するクライアントのユーザが変更できる情報をユーザ定義パラメータ415に定義する。図6のアクセス制御パラメータ412では、3行目から4行目で商品名に対するサーバ定義パラメータ、5行目で数量に対するサーバ定義パラメータ、6行目で配送先に対するサーバ定義パラメータをそれぞれ定義している。また、10行目で商品名に対するユーザ定義パラメータ、11行目で数量に対するユーザ定義パラメータ、14行目で配送先に対するユーザ定義パラメータを定義している。また、ユーザ定義パラメータ415では、商品入力、配送先入力という新たなタグを追加して、各入力項目をカテゴリ分けしている。すなわち商品入力というカテゴリには、商品名と数量という2つの入力項目を定義し、前記2つの入力項目の入力担当者として山田花子を商品入力タグの属性として定義している。同様に配送先入力というカテゴリには、配送先という入力項目を定義している。

【0023】ステップ1102では、ユーザ定義パラメータ415にセキュリティタグコードを付加し、ユーザ定義パラメータ415の変更権限者を定義して、ユーザ定義パラメータタグの属性として付加する。図6において、セキュリティタグコードは、8行目に記述された「変更担当＝「佐藤一郎」」である。

【0024】ステップ1103では、アクセス制御パラメータ412において、サーバ定義パラメータ414と、ユーザ定義パラメータ415についてそれぞれハッシュ値を計算し、記憶装置112に保存する。また、当該ハッシュ値それぞれに電子署名を作成し、それぞれをサーバ定義保護情報418と、ユーザ定義保護情報419に付加する。具体的には、処理機構22で、サーバ定義パラメータ414について、一方向関数を用いてハッシュ値を計算して求め、その値を記憶装置112に保存

する。また、当該ハッシュ値に対して記憶装置112に保存されているサーバ11の秘密鍵で暗号化し署名を作成する。これをサーバ定義保護情報418に付加する。同様に、処理機構22で、ユーザ定義パラメータ415について、一方向関数を用いてハッシュ値を計算し、その値を記憶装置112に保存する。また、当該ハッシュ値に対して記憶装置112に保存されているサーバ11の秘密鍵で暗号化し電子署名を作成する。これをユーザ定義保護情報419に付加する。ステップ1101からステップ1103の処理により、あらかじめ帳票テンプレート1つ以上作成しておき、記憶装置112にあらかじめ保存しておく。

【0025】ステップ1201及びステップ1104では、クライアント12のユーザは、入力装置121から入力する帳票テンプレートをサーバにおいて検索するための検索条件を、通信機構31を通じてサーバ11の通信機構21に送信する。サーバ11の処理機構22は、クライアント12から送られた帳票テンプレートの検索条件をもとに、記憶装置112の中から帳票テンプレートを検索し、対応する帳票テンプレート41を通信機構21を通じて、クライアントの通信機構31へ送信する。クライアントの処理機構32は、通信機構31が受信した帳票テンプレート41を取得する。

【0026】ステップ1202では、ユーザからのユーザ定義パラメータ415の変更要求があれば、クライアント12の計算機122の処理機構32は解析機構33を通じて帳票テンプレート41を解析して、帳票テンプレート41のユーザ定義パラメータ415に定義している変更権所有者と、ユーザが入力装置121から入力するユーザに関するユーザ情報を比較して、ユーザがユーザ定義パラメータ415の変更権を所有しているか確認し、変更権を所有していない場合は変更を受け付けずに、ステップ1204に行く。変更権を所有している場合はユーザ定義パラメータ415の変更を受け付ける。この際、処理機構32は変更したユーザ定義パラメータ415が、サーバ定義パラメータ414と矛盾してないかまた、サーバのデータベースにアクセスするように変更されていないかを監視し、矛盾が生じた場合は変更を無効にする。

【0027】図9に、本実施形態により変更されたアクセス制御パラメータ412を示す。9行目で商品入力カテゴリの入力担当者が佐藤一郎に、13行目で配送先入力カテゴリの入力担当者が鈴木太郎に、14行目で配送先のデータ型512が選択に、入力DB513が資材に、入力レコード514が配送先に変更されている。このように、データの参照先として、サーバ11上のデータベースは指定することはできないが、クライアント12のローカルにあるデータベースは、ユーザ定義パラメータ415に指定することができる。

【0028】ステップ1203では、処理機構32が、

更新したユーザ定義パラメータ415について一方向関数でハッシュ値を計算して、その値に対して記憶装置124に保存されているユーザ定義パラメータ415の変更者の秘密鍵で暗号化し電子署名を作成する。これをユーザ定義保護情報419に書き込む。

【0029】ステップ1204では、ユーザからのデータ入力（更新）の要求があれば、処理機構32は解析機構33を通じて帳票テンプレート41を解析して、帳票テンプレート41のユーザ定義パラメータ415に定義している入力担当者と、ユーザが入力装置121から入力するユーザに関するユーザ情報を比較して、ユーザがデータ領域411への入力権（更新権）を所有しているか確認し、入力権を所有していない場合は変更を受け付けずに、ステップ1206に行く。入力権を所有している場合は、帳票テンプレート41に定義している各入力項目のデータ型を解析機構33が解析し、処理機構32が各入力項目毎に対応した入力フォームを、記憶装置124に保存されている入力画面のGUIライブラリより取得し、表示装置123に入力画面を作成、表示して、入力権を所有しているデータ領域411への入力を受け付ける。

【0030】図10は、本実施形態によって作成された、表示装置123に表示された入力画面61である。図9の最新のアクセス制御パラメータ412を見ると、3行目より商品名のデータ型は選択、5行目より数量のデータ型は数値であるので、それぞれ選択フォーム62、数値フォーム63が画面上に作成される。配送先に関しては13行目より、現在のユーザに入力の権限が与えられていないので、入力ができないように入力フォームを作成しない。このようにして作成された入力画面をもとに、ユーザは入力の権限が与えられた入力項目に対して入力を行い、処理機構32はユーザの入力データを解析機構33を通して、帳票テンプレート41のデータ領域411の対応するタグの値として保存する。その際、処理機構32は、ユーザが無効な入力をしていないかどうかを、解析機構33を通してアクセス制御パラメータ412とユーザの入力データとを比較し、ユーザの無効な入力を受け付けないようにする。なお、本実施形態では、ユーザ定義パラメータに入力権を設定できることは記載されているが、入力権の他に参照権を設定することもできる。この場合、参照権のないデータは画面上に表示されない。

【0031】ユーザが入力を終え、登録ボタン65を押下したら、入力受付を終了しステップ1205へ進む。また、図9のアクセス制御パラメータの3行目には、商品名はカタログデータベースの商品名というレコードから選択するように定義している。このカタログデータベースがサーバにあるとすると、クライアント12は、サーバ11にデータベースへのアクセスを要求する必要がある。このように処理の途中でサーバとの更新が必要と

なった場合も、入力処理を中止しステップ1205に進む。

【0032】ステップ1205では、ユーザが更新した帳票入力データについて、処理装置32が一方関数でハッシュ値を計算し、その値に対して記憶装置124に保存されているデータ領域411の入力データ変更者の秘密鍵で暗号化し電子署名を作成する。これをデータ保護情報417に書き込む。

【0033】ステップ1206では、処理機構32が記憶装置124に保存されているサーバ11の公開鍵で、サーバ定義保護情報418に定義されているサーバ定義パラメータ414の電子署名を復号化し、サーバ定義パラメータ414のハッシュ値を計算したものと比較し、サーバ定義パラメータが改ざんされていないか確認する。

【0034】次に、処理機構32が記憶装置124に保存されているユーザ定義パラメータ415の変更権所有者の公開鍵で、ユーザ定義保護情報419に定義されているユーザ定義パラメータ415の電子署名を復号化し、ユーザ定義パラメータ415のハッシュ値を計算したものと比較し、ユーザ定義パラメータが改ざんされていないか確認する。また、処理機構32が、解析機構33を通じて、データ領域411のデータが、アクセス制御パラメータ412に定義しているパラメータと比較して有効であるか確認する。サーバ定義パラメータ414の非改ざん性、ユーザ定義パラメータ415の非改ざん性、データ領域の411の正当性がすべて確認されたら、ステップ1207に進む。上記説明における公開鍵、秘密鍵は既に公知になっている公開鍵、秘密鍵と同様のものであるため、公開鍵、秘密鍵についての説明は省略する。

【0035】ステップ1207とステップ1105では、処理機構32が通信機構31を通じて帳票テンプレート41をサーバ11に送信し、サーバ11の処理機構22は通信機構21を通じて帳票テンプレートを取得する。

【0036】ステップ1106では、処理機構22が記憶装置112に保存されているサーバ11の公開鍵で、サーバ定義保護情報418に定義されているサーバ定義パラメータ414の電子署名を復号化し、ステップ1102で記憶装置112に保存していた当該ハッシュ値と比較し、サーバ定義パラメータが改ざんされていないか確認する。次に、処理機構22が記憶装置112に保存されているユーザ定義パラメータ415の変更権所有者の公開鍵で、ユーザ定義保護情報419に定義されているユーザ定義パラメータ415の電子署名を復号化し、ユーザ定義パラメータ415のハッシュ値を計算したものと比較し、ユーザ定義パラメータが改ざんされていないか確認する。また、処理機構22が、解析機構23を通じて、データ領域411のデータが、アクセス制御パ

ラメータ412に定義しているパラメータと比較して有効であるか確認する。サーバ定義パラメータ414の非改ざん性、ユーザ定義パラメータ415の非改ざん性、データ領域の411の正当性がすべて確認されたら、ステップ1107に進む。なお、ステップ1206とステップ1106は同じ処理を行っているため、どちらか一方を省略することも可能である。

【0037】ステップ1107では、処理機構22が文書保護情報417に定義されているデータ領域411の電子署名を、記憶装置112に保存されているユーザ定義パラメータ415で定義されているそれぞれの入力担当者の公開鍵で復号化し、データ領域411の入力データのハッシュ値を計算したものと比較し、データ領域411がアクセス制御パラメータ412で定義された入力担当者によって入力されたかどうか確認する。

【0038】ステップ1108では、処理機構22がデータベース管理機構24を通じて、アクセス制御パラメータ412を用いて、データ領域411の更新内容をもとに業務データベース113の内容を更新したり、業務データベース113からデータを読み出す。業務データベース113からのデータの読み出し処理は、例えば、ステップ1204で、商品名の選択肢をカタログデータベースの商品名レコードから読み出すというクライアント12からの要求に対して、対応するデータベースからデータを読み込む処理である。

【0039】ステップ1109とステップ1208では、ステップ1108で処理した結果を通信機構21を通じてクライアント12に送信し、処理機構32は通信機構31を通じて処理結果を受信する。

【0040】ステップ1209では、ステップ1203で登録ボタン55が押下されていたら、処理を終了する。それ以外の場合、すなわち、ステップ1204の処理の途中でサーバとの通信が必要になり、サーバとの通信結果が受信された場合にはステップ1204に戻る。サーバとの通信結果が受信された場合、例えば、ステップ1204における商品名の選択肢をサーバ11の業務データベースから読み込んだデータを受信した場合には、この受信データをもとに、処理機構32が表示装置123に商品名の選択肢を表示させる。この画面表示を図11に示す。サーバ定義パラメータ414に従って、カタログデータベースの商品名から読み出してきた、商品名の選択肢がノートパソコン、エアコン、電子レンジであるとする画面表示は67のようになる。

【0041】

【発明の効果】以上述べたように、本発明によれば、帳票の入力データと業務データベースのレコードの読み出しと更新を制御するアクセス制御パラメータを、サーバ側で定義するパラメータとクライアント側で定義変更できるパラメータとに分け、それぞれに署名を付加することにより、アクセス制御パラメータを不正に改ざんし

て、データベースにアクセスすることを防止することが可能となる。また、クライアント側でパラメータを変更することができることにより、より柔軟な電子帳票処理が可能となる。

【図面の簡単な説明】

【図1】本発明の電子帳票処理方法の実施例の処理手順のフローチャートを示す図である。

【図2】本発明の適用される電子帳票処理システムの全体構成を示す図である。

【図3】サーバのモジュール構成を示す図である。

【図4】クライアントのモジュール構成を示す図である。

【図5】電子帳票テンプレートの構成を示す図である。

【図6】アクセス制御パラメータの構成を示す図である。

【図7】文書保護情報の構成を示す図である。

【図8】アクセス制御パラメータのテーブル構成図であ

る。

【図9】クライアントのユーザがユーザ定義パラメータを変更した後のアクセス制御パラメータの構成を示す図である。

【図10】初期帳票入力画面を示す図である。

【図11】入力項目の選択肢をサーバから読み出してきた後の帳票入力画面を示す図である。

【符号の説明】

11 サーバ

12 クライアント

13 通信ネットワーク

111、122 計算機

112、124 記憶装置

113 業務データベース

121 入力装置

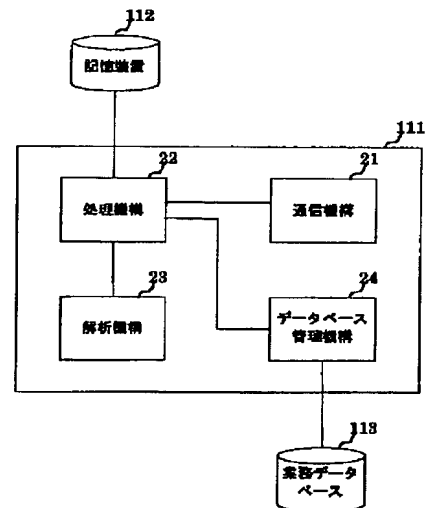
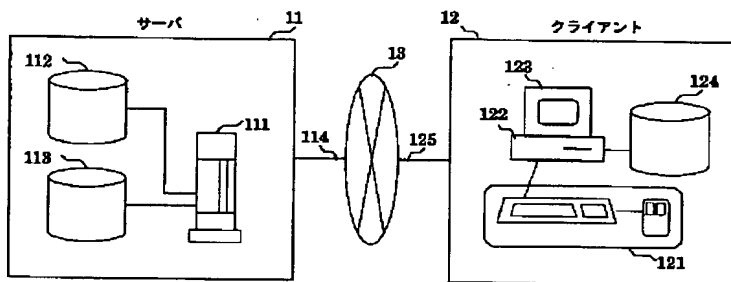
123 表示装置

【図2】

【図3】

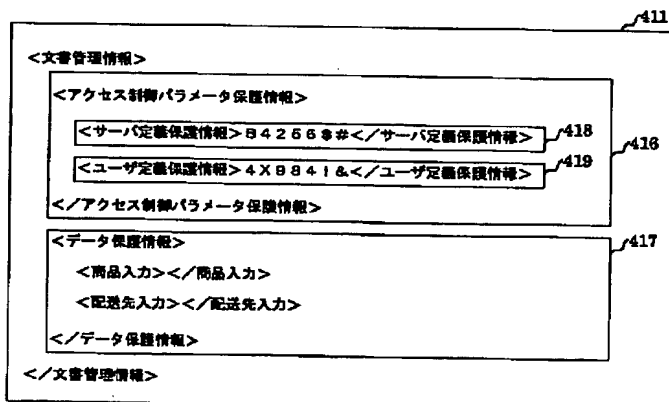
【図2】

【図3】



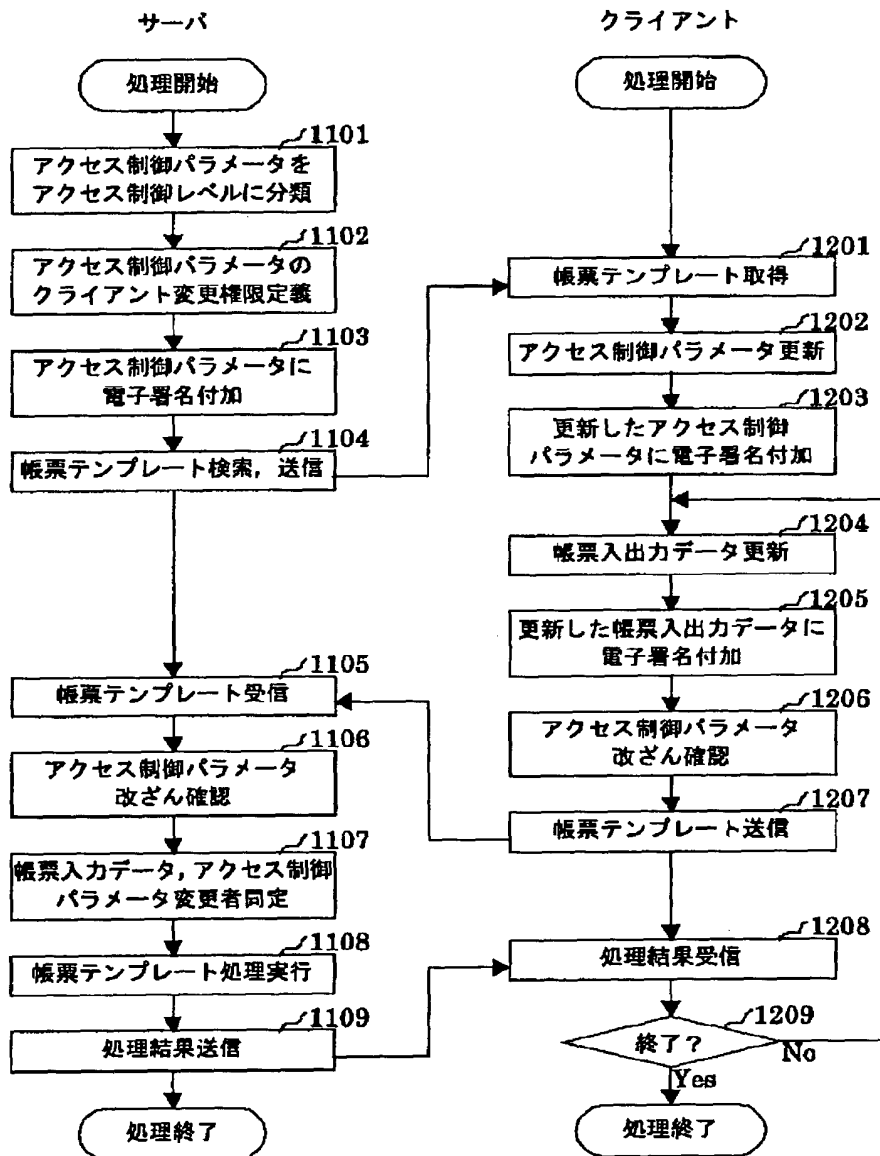
【図7】

【図7】



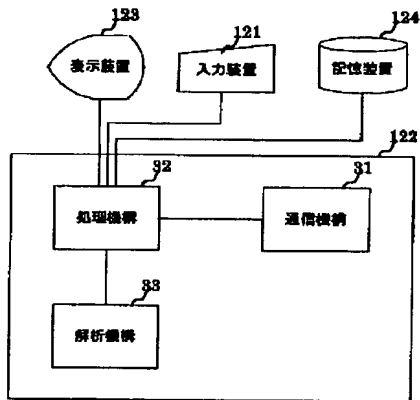
【図1】

【図1】



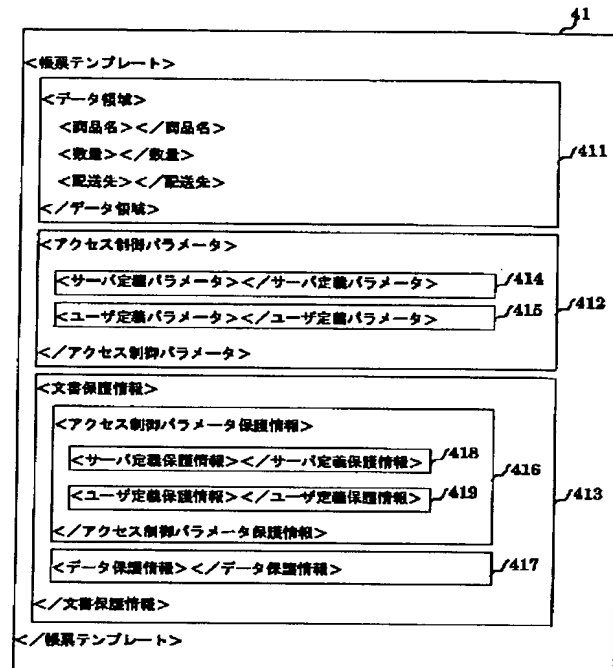
【図4】

【図4】



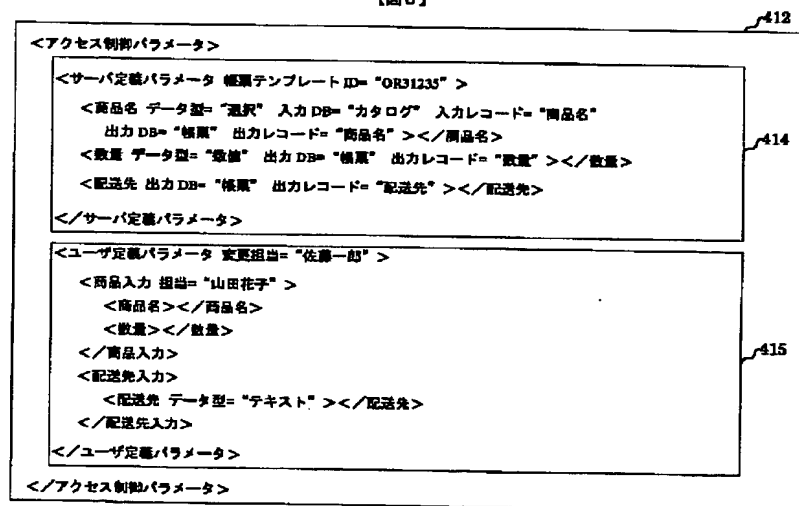
【図5】

【図5】



【図6】

【図6】



【図8】

【図8】

412 入力項目名	511 データ型	512 入力DB	513 入力レコード	514 出力DB	515 出力レコード
商品名	選択	カタログ	商品名	帳票	商品名
数量	数値	——	——	帳票	数量
配送先	テキスト	——	——	帳票	配送先

【図9】

【図9】

412

<アクセス制御パラメータ>

<サーバ定義パラメータ 帳票テンプレートID= "OR31235" >

<商品名 データ型= "選択" 入力DB= "カタログ" 入力レコード= "商品名"
出力DB= "帳票" 出力レコード= "商品名" ></商品名>

<数量 データ型= "数値" 出力DB= "帳票" 出力レコード= "数量" ></数量>

<配送先 出力DB= "帳票" 出力レコード= "配送先" ></配送先>

</サーバ定義パラメータ>

<ユーザ定義パラメータ 変更担当= "佐藤一郎" >

<商品入力 担当= "佐藤一郎" >

<商品名></商品名>

<数量></数量>

</商品入力>

<配送先入力 担当= "鈴木太郎" >

<配送先 データ型= "選択" 入力DB= "資料" 入力レコード= "配送先" ></配送先>

</配送先入力>

</ユーザ定義パラメータ>

</アクセス制御パラメータ>

414

415

【図10】

【図10】

61

注文書作成

商品名 :

数量 :

配送先 :

62

63

64

65

66

確定

キャンセル

【図11】

【図11】

61

注文書作成

商品名 :

数量 :

配送先 :

62

63

64

65

66

確定

キャンセル

フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	ターム(参考)
G 0 6 F	17/30	G 0 6 F 15/40	3 1 0 F
			3 2 0 B
			3 7 0 Z
		15/401	3 4 0 A
(72) 発明者	横村 克也	F ターム(参考)	5B075 KK03 KK07 KK13 KK33 KK37
	神奈川県川崎市麻生区王禅寺1099番地 株		KK40 KK43 KK54 KK63 KK66
	式会社日立製作所システム開発研究所内		ND03 ND20 ND23 NK10 NK45
			NK46 PP30 PQ02 PQ05 UU38
			5B082 AA11 EA11 EA12 GA02 GA13
			GA14 GC02 GC04 GC05
			5B089 GA11 GA21 JA08 JB22 KA07
			KA10 KA17 KB10 KC58 KH30